Assignment V
Next Generation Firewall (NGFW)
pfSense / OPNsense

S7 / S5 B.Tech: Computer Security Lab

Due Date: 27 October 2021 11:30 PM

1 Introduction

A next-generation firewall (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall. While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

1.1 next-generation firewall

A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules. A next-generation firewall (NGFW) does this, and so much more. In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to Gartner's definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Threat intelligence sources
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

The best next-generation firewalls deliver five core benefits to organizations, from SMBs to enterprises. Make sure your NGFW delivers:

1. Breach prevention and advanced security

   The No. 1 job of a firewall should be to prevent breaches and keep your organization safe. But since preventive measures will never be 100 percent effective, your firewall should also have advanced capabilities to quickly detect advanced malware if it evades your front-line defenses. Invest in a firewall with the following capabilities:

   - Prevention to stop attacks before they get inside
   - A best-of-breed next-generation IPS built-in to spot stealthy threats and stop them fast
   - URL filtering to enforce policies on hundreds of millions of URLs
   - Built-in sandboxing and advanced malware protection that continuously analyzes file behavior to quickly detect and eliminate threats
   - A world-class threat intelligence organization that provides the firewall with the latest intelligence to stop emerging threats

2. Comprehensive network visibility

   You can't protect against what you can't see. You need to monitor what is happening on your network at all times so you can spot bad behavior and stop it fast. Your firewall should provide a holistic view of activity and full contextual awareness to see:

   - Threat activity across users, hosts, networks, and devices
   - Where and when a threat originated, where else it has been across your extended network, and what it is doing now
   - Active applications and websites
   - Communications between virtual machines, file transfers, and more

3. Flexible management and deployment options

   Whether you are a small to medium-sized business or a large enterprise, your firewall should meet your unique requirements:

   - Management for every use case-choose from an on-box manager or centralized management across all appliances
   - Deploy on-premises or in the cloud via a virtual firewall
   - Customize with features that meet your needs–simply turn on subscriptions to get advanced capabilities
   - Choose from a wide range of throughput speeds

4. Fastest time to detection

   The current industry standard time to detect a threat is between 100 to 200 days; that is far too long. A next-generation firewall should be able to:

   - Detect threats in seconds
   - Detect the presence of a successful breach within hours or minutes
   - Prioritize alerts so you can take swift and precise action to eliminate threats
   - Make your life easier by deploying consistent policy that's easy to maintain, with automatic enforcement across all the different facets of your organization

5. Automation and product integrations

   Your next-generation firewall should not be a siloed tool. It should communicate and work together with the rest of your security architecture. Choose a firewall that:

   - Seamlessly integrates with other tools from the same vendor
   - Automatically shares threat information, event data, policy, and contextual information with email, web, endpoint, and network security tools
   - Automates security tasks like impact assessment, policy management and tuning, and user identification

2 Opensource Firewall: m0n0wall / pfSense / OPNsense

m0n0wall was an embedded firewall distribution of FreeBSD, one of the BSD operating system descendants. It provides a small image which can be put on Compact Flash cards as well as on CD-ROMs and hard disks. It runs on a number of embedded platforms and generic PCs.

pfSense is a firewall/router computer software distribution based on FreeBSD. The open source pfSense Community Edition and pfSense Plus is installed on a physical computer or a virtual machine to make a dedicated firewall/router for a network.

OPNsense is an open source, FreeBSD-based firewall and routing software developed by Deciso, a company in the Netherlands that makes hardware and sells support packages for OPNsense. It is a fork of pfSense, which in turn was forked from m0n0wall, which was built on FreeBSD. It was launched in January 2015.

3 What you have to do?

1. Install pfSense in a virtual box as Virtual Machine (VM) with 1GB RAM and two virtual NIC Card and make the connections as given in the diagram bellow. Refer pfSense Documentation link given in Reference 5 for installation and configuration details.

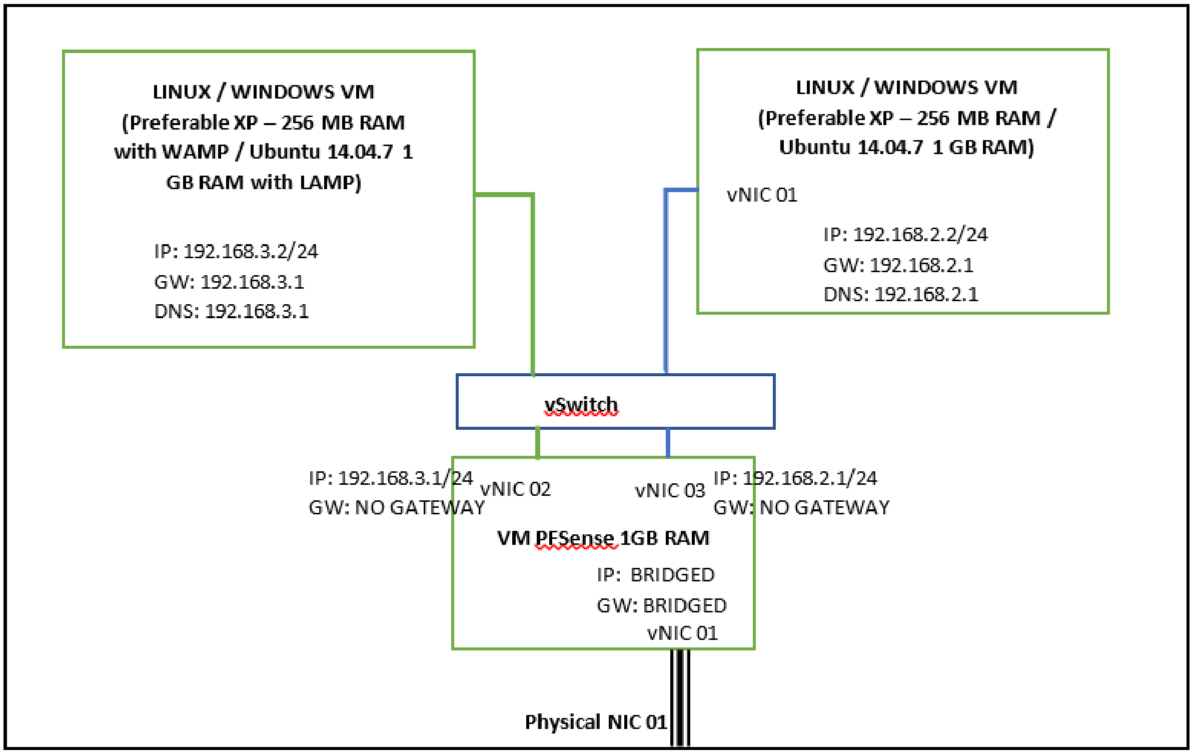

Figure 1: Network Diagram

2. As shown in the diagram, install a management PC and a client PC both as VMs. Please install an operating system which takes very less RAM (may be 256 MB RAM / 1GB RAM each) in both the machines. Name one as management PC and other as Client PC. Install Apache PHP mySQL and load DVWA into the client PC. Enable network access for DVWA, and access it from your Management PC (After configuring the network as given in the Figure 1.)

3. Configure the NTP Server, in pfSense by setting the public DNS Server

4. Configure the basic firewall by referring ”Managing Firewall Rules” from

pfSense documentation. Make sure you are getting internet access in both management and client PC. [http://IPADDRESS/firewall_rules.php]

5. Block internet access for client PC and allow internet access only for management PC.

6. Configure “traffic shaper” (Reference 7) to restrict/limit the internet access and speed to the client VM.

7. Configure “Captive Portal” (Reference 6) to enable it and create login portal for client to access internet. The ”Captive Portal” configuration has to be customised to load your image as logo in the login page.

8. Install ”pfBlocker-NG Package” (Reference 9) by going to package manager given in (Reference 8). Configure the package, by getting ” MaxMind License Key” (free user), and loading the geoIP information from that. Understand what is use of package ”pfBlocker-NG” and ”DNSBL”. What is its use? How it works?

9. Add an IP from your Bridged network and configure it as ”Virtual IP”. Now Using NAT, setup the client system as Server, which is accessible from your Laptop host Operating System. In this process you are actually hosting an internal server to public domain using a Firewall. This is optional and will be given extra credits, if done and demonstrated.

4 What you have submit?

Google drive URL of a single recorded video. The video should be having demonstration along with audio commentary, for each of the above task.

You can do all the above activities in OPNSense also. So if someone feels to do it in OPNSense, then they are free to do the same using OPNSense instead of pfSense, and could submit the recorded video from OPNSense.

Any clarifications regarding the assignment has to brought to the instructor by 20/10/2021.

5 Prerequisite for Assignment VI

Preserve the VMs and configurations done for doing Assignment VI.

6 Readings

1. What Is a Next-Generation Firewall?.

2. m0n0wall.

3. pfSense
4. OPNsense
5. pfSense Documentation
6. Captive Portal
7. Traffic Shaper
8. Package Manager
9. pfBlocker-NG Package